SCGA
The Scottish Council on Global Affairs

REGULATING RANSOMWARE THROUGH INTERNATIONAL LAW

A SCOTTISH COUNCIL ON GLOBAL AFFAIRS REPORT

January 2024

TSVETELINA VAN BENTHEM & CHRISTIAN J. TAMS

scga.scot
@scga_scot

THE PROJECT

This Report addresses the application of international law to ransomware operations. It analyses substantive rules relevant to ransomware and outlines how states violating these rules can be held accountable. Its central aim is to highlight the applicable legal regimes and the main interpretative controversies concerning the boundaries of legal rules. The analysis offered in this Report will inform debates between stakeholders about ways of countering the ransomware threat through international law, and inform practically-relevant responses.

This Report has benefited from discussion at two roundtables involving members of government, industry and academia, and from consultations with the insurance sector.

The preparation of this Report has been supported by funding from the Foreign, Commonwealth and Development Office (FCDO), as part of its commitment to support the work of the SCGA as a non-partisan think tank based in Scotland.

This Report has been prepared by the authors in their personal capacity. Views and opinions expressed in the Report are those of the authors. They do not necessarily reflect the views of the FCDO or the SCGA.

"Ransomware is one of the most pressing geopolitical and security concerns of the decade.

International law can play an important role in countering the ransomware threat."

Part I.

The ransomware threat and international law

On 18 March 2021, an employee at the Irish Health Service Executive (HSE) opened a spreadsheet they had received by email, unwittingly setting in motion a chain of events that disrupted the provision of healthcare and the operation of digital systems of the HSE for months to come.[1] Opportunities to detect the hackers were missed, and a subsequent investigation found that HSE systems were vulnerable to cyber intrusion.[2] Once the hackers encrypted the data and locked the HSE out of its systems, medical personnel lost access to patient information, as well as to systems for clinical care. This is not an isolated incident. Ransomware deployed against London's Hackney Council – a Council responsible for the lives of more than 250,000 people – affected people's health, housing and finances.[3] A suspected ransomware attack affected City of London traders at the start of February 2023, requiring the disconnecting of servers.[4] The list goes on, with reports of ransomware incidents piling every day.

These ransomware incidents illustrate that key digital systems, both public and private, are vulnerable to cyber intrusion, and that the price of such intrusions can be very high. Malicious actors – individuals, criminal groups and states – can, and do, take advantage of such vulnerabilities, exploiting them for monetary and political gain. The threat of ransomware cuts across territorial borders and, because of the inter-connectedness of digital systems, vulnerabilities in networks located in one country can affect another directly, even on the other side of the globe.

Vulnerability calls for resilience-building; the varied ransomware-related harms call for the protection of both individual and state interests; and the cross-border nature of the threat calls for multilateral responses. International law provides a legal framework for addressing the global threat of ransomware. It is one tool available to decision-makers in crafting their responses to ransomware operations. It is significant because it lays down binding rules against which state conduct can be assessed and determines how unlawful conduct can be addressed.

The following sections of the Report review, first, the contemporary ransomware threat landscape, and second, the importance of international law as a framework for addressing ransomware operations.

The threat of ransomware cuts across territorial borders and, because of the inter-connectedness of digital systems, vulnerabilities in networks located in one country can affect another directly, even on the other side of the globe.

1. The ransomware threat landscape

Recent years have seen a tidal wave of ransomware operations. This wave, sweeping across regions and sectors, is causing long-lasting economic and security consequences, exploiting existing vulnerabilities and creating new ones. Its reach transcends borders, and its impact is capable of destabilising governments and the private sector. Ransomware is described as 'one of the most significant and growing international cyber threats',[5] a 'widespread form of cybercrime that [...] has become a serious national security threat and a public health and safety concern'.[6] The October 2022 INTERPOL Global Crime Trend Summary Report identified ransomware as the cybercrime attracting the highest threat level according to member states of the organisation, and one for which expectations are of further escalation and spread in the coming three to five years.[7]

The effects of ransomware operations are both tangible and debilitating. Just in the past year, a ransomware operation on software supplier Advanced disrupted the NHS, reportedly causing widespread outages, affecting ambulance dispatch and mental health services, among others.[8] In the spring of 2022, Costa Rica came under a steady stream of ransomware operations impairing its delivery of essential services, prompting the government to declare a state of emergency.[9] Other major incidents from 2022 disrupted an Indian airline, detention centres in the United States, and private companies.[10] As regards targeted countries, **the United Kingdom ranks third**, following closely after the United States and Canada.[11]

Ransomware operations are not simply increasing in frequency and reach. They are becoming more sophisticated, distributed across actors, and professionalised, as the ransomware 'ecosystem' evolves. To begin with, **ransomware can be defined as a type of malware that prevents a user from accessing their device and the data stored on the device, usually through the encryption of files.**[12] The system or data remain locked until a demand is met.[13] While initially, ransomware was operated by single groups developing and injecting the payload in the victim's system, recent years have seen a concerning trend towards a 'ransomware as a service' model. Under this model, different groups may be in charge of the development of the payload, data leakage extortions, provision of access to compromised accounts. Another worrying trend is the practice of double extortion

whereby perpetrators first exfiltrate and encrypt data, and then post or threaten to post the data as a pressure point to secure the ransom payment.[14]

Non-state criminal groups carry out the clear majority of ransomware operations. Conti, REvil, BlackCat, Hive and Black Basta – all criminal organisations specialising in ransomware – are names that regularly appear in the news.[15] Law enforcement agencies have recently made great strides in dismantling, or at least disrupting the operation of criminal groups. In early 2023, it was reported that an FBI operation against Hive both stole decryption keys from the group and took down its website and channels for communication.[16] However, the sheer number of criminal organisations operating in cyberspace, and their swift adjustments to regulatory and enforcement tactics, make the threat particularly hard to address. Beyond non-state criminals, **state actors are also reportedly involved in ransomware operations**,[17] be it through their own agencies or by directing and controlling the operations of private actors.

Clearly, then, ransomware is one of the most pressing geopolitical and security concerns of the decade. How have states and other stakeholders responded to the rise of ransomware?

The threat posed by ransomware is well understood across governments and the private sector. In November 2022, the International Counter Ransomware Initiative issued a Joint Statement, reaffirming the commitment of its member states to resilience-building and coordination efforts in curbing the ransomware threat.[18] The G7 has set up the Cyber Expert Group, which has called for intensified efforts to tackle ransomware operations, and recently published two reports on ransomware and third-party risk.[19] Domestic institutions also seek to grapple with the means, methods and effects of ransomware operations. Ransomware features in the 2022 United Kingdom National Cyber Security Strategy[20] and constitutes an important strand of the work of the National Cyber Security Centre,[21] including through the creation of a ransomware hub.[22] In April 2023, the United Kingdom Government launched GovAssure, a cyber security scheme to review, assess and enhance the cyber security of government departments that run key services for the public.[23]

The **insurance industry** is adding its own voice to the conversation, publicising its cybersecurity advice to clients and seeking to carve out exceptions from insurance coverage to tackle the risk of exorbitant cyber-related claims. In late 2022, Allianz in its report 'Cyber: The changing threat landscape' provided an overview of the changes in ransomware models, and the impact of regulatory and cybersecurity measures on cyber ransomware criminality.[24] Also in 2022, Lloyd's announced a carveout of insurance coverage for both war and non-war state-backed cyber attacks with catastrophic effects.[25] This measure was taken to counter the systemic risk faced by insurers from claims arising out of such operations.

Increasingly, the insurance industry has been publicising its cybersecurity advice to clients and seeking to carve out exceptions from insurance coverage to tackle the risk of exorbitant cyber-related claims.

Research institutions are bringing their expertise to the technical, legal and policy discussions on ransomware. For instance, in 2021, the Oxford Institute for Ethics, Law and Armed Conflict, as part of the Oxford Process on International Law Protections in Cyberspace, issued a statement on the regulation of ransomware operations, outlining a short list of consensus protections under existing international law.[26] In July 2023, the Royal United Services Institute published *Cyber Insurance and the Ransomware Challenge*, an occasional paper outlining, among others, the potential of cyber insurance to disrupt the ransomware criminal enterprise.[27]

The ransomware threat and the insurance industry

The insurance industry trades with risk. For a premium paid by clients, insurers assume the risk of larger losses. Certain types of risk, however, are of a magnitude capable of destabilising the insurance market, with anticipated losses that the insurance industry is unable to absorb. These types of risk relate to extreme events and are handled through exclusion clauses established in insurance contracts. Exclusion clauses related to acts of war are a common example of such coverage carveouts.

Cyber operations, and in particular ransomware, generate significant financial losses for the private sector. As clients are seeking to cover the risk of ransomware operations through insurance, insurers must decide which types of cyber risk are acceptable to them, and, for those deemed unacceptable, how exclusion clauses could be drafted.

In August 2022, Lloyd's issued a Market Bulletin that considered the possible exclusion of state-sponsored cyber operations from insurance coverage. According to the Bulletin, 'when writing cyber-attack risks, underwriters need to take account of the possibility that state backed attacks may occur outside of a war involving physical force. The damage that these attacks can cause and their ability to spread creates a similar systemic risk to insurers.' Further, the requirement for exclusions in standalone cyber-attack policies relates to the exclusion of losses 'from state backed cyber-attacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state.' This may indicate that the required exclusions do not apply to any state-backed operation, but only to those that reach a certain magnitude of effects. This would align with the goal of managing extreme risk. Exclusions that extend to *any cyber operation* supported by a state would indeed seem misaligned with this goal – the catastrophic effects of a cyber operation are not contingent on state involvement. In fact, the harms that non-state-affiliated criminal groups can produce could well be more significant than those within the capacity of most states. What matters for the purposes of managing exposure risk is the size of the cyber event, not its author.

A central aim of the insurance industry is to limit exposure through well-crafted exclusions. Well-crafted insurance exclusions are those that are necessary for achieving the goal of the carveout without unduly limiting coverage, that are understandable to the clients, and that navigate legal terminology without causing confusion. For instance, it is unclear whether the references to 'state-sponsored' cyber operations refer to the tests of legal attribution of conduct to a state, as understood in international law, are broader and encompass acts of state complicity in the conduct of non-state actors or have a self-standing contractual meaning that does not track notions of attribution or complicity in international law.

Another consideration related to ransomware operations that complicates the analysis for insurers is that the insurance paid to clients could subsequently be used to pay ransom to groups that are under domestic or international sanctions regimes. Although the insurance industry does not favour a blanket prohibition on the payment of ransom, the area of ransom payments is not one of complete freedom. When the group or activity that the ransom would foreseeably sponsor falls within sanctioned categories, domestic and international law may impose limitations on ransom payments.

The insurance market is still trying to come to grips with the new realities of cyber criminality. Given the scale of economic losses already produced by ransomware, and the potential for ransomware operations to cripple entire sectors of critical national infrastructure, losses may become harder to absorb by the insurance industry alone. Alternative options can be considered. The model used by Pool Reinsurance, UK's largest terrorism reinsurer, may be instructive. Pool Re was founded by the insurance industry in cooperation with the UK government, and is supported by unparalleled financial security as a result of the unlimited HM Treasury guarantee. A similar model could be used for catastrophic cyber operations, with losses covered to a point by the insurance industry and backed above that point by governments. One difficulty with ransomware is the direction in which the insurance money would then flow – the payment of ransom to certain criminal groups would become an even more sensitive matter if government funds are involved.

The ransomware threat landscape is expanding, evolving, and reshaping itself to the regulatory and enforcement climate. At the same time, states have shown a strong commitment to countering the operations of ransomware groups, including through multilateral cooperation efforts, technical capacity-building and the clarification and development of international law. It is to the significance of international law frameworks that the remainder of this section turns.

2. Tackling the ransomware threat through international law

To tackle ransomware criminality, states, the private sector and other entities and institutions need to bolster their technical and organisational capacity, collaborate with the relevant authorities, and aim to strengthen domestic regulatory responses. Given that technical, organisational and domestic legal responses are already being deployed to counter ransomware operations, what is the benefit of adding an international law dimension, and allocating financial and personal resources to the clarification and development of the international legal framework? The answer to this question can be divided into three parts – the regulatory need, the deterrence effect of clear rules, and the avenues for responding to breaches.

First, the transnational operation of criminal ransomware groups and the interconnectedness of digital networks necessitate **regulatory responses taken at the inter-state level**. No state can counter the ransomware threat on its own. Thus, any meaningful approach to this threat has to be grounded in obligations, both negative and positive, that require a certain conduct of all, or at least a wide majority of, states. International law provides a common language between states: it can ensure a framework for predictable interactions between actors, and institutional platforms for multilateral dialogue. Grounding the discussion on ransomware in international law does not imply an adversarial nature to this discussion. Rather, it can be structured around cooperation in the specification and development of rules that accommodate diverging state needs, account for differentiated capacities, and entrench avenues for collaboration through legal and technical capacity-building. Such efforts are already underway at the United Nations and other multilateral fora.

Second, clear international legal rules can **deter harmful conduct** and incentivise the taking of positive measures at the domestic level. Many forms of state conduct carried out through information and communications technologies (ICTs) inhabit a grey area of uncertain legality, as the elements of the relevant international rules remain contested between states. The need for clarity is well understood. In recent years, states have publicised their national positions on the application of international law to cyberspace, proffering their positions on the key applicable rules and their elements. This clarification is also important for the private sector, as insurance companies, in considering insurance coverage, may rely on terms and doctrines taken from international law, such as 'act of state' or 'act of war'.

Clarification is particularly relevant in the field of positive obligations, where states enjoy a certain discretion in the ways in which they can discharge their duties. Collections of existing legal, technical, organisational and cooperation measures can both help specify the precise contours of positive obligations and act as a repository of best practices for the purposes of capacity and confidence building.

Third, framing claims in the language of international law opens the possibility of **invoking responsibility** and demanding reparation, as well as enforcing obligations in cases of non-compliance. International law tells us which states are injured by particular internationally wrongful acts, and which injured and non-injured states can invoke the responsibility of the wrongdoer.[28] Depending on the rule that has been breached, international law may provide avenues for adjudication and review. The responsible state owes reparation and may be required to provide guarantees of non-repetition.[29] A finding of a violation may entail significant reputational costs for states, designating them as untrustworthy international partners. And finally, given that there is no central and general enforcement authority in the international system, international law allows decentralised enforcement through countermeasures – a doctrine wide enough to allow the exercise of meaningful pressure to induce compliance, and circumscribed enough to minimise the risk of abuse.[30]

As is clear from the current debate, international law provides a language for the articulation of claims and cooperation efforts.[31] States and other stakeholders have, in recent years, pushed the international law agenda in significant ways. Through national

positions, reports, manuals and statements, they have sought to clarify the scope of existing international law. And through multilateral negotiations, they have initiated the development of new rules in areas that require strong harmonisation and cooperation, such as the field of cybercrime.

Because international law is a prominent aspect of the inter-governmental discussions at the United Nations, both within the groups dealing with ICTs in the area of international peace and security and those tasked with the elaboration of a cybercrime instrument, **the time to voice national positions** on the content of customary international law and provisions of negotiated treaties **is now**. The law is being shaped in the discussions and negotiations, and states that remain silent risk losing influence over the direction of international legal regulation in this area. Of course, the capacity to meaningfully engage in international law-making depends on the availability of legal and technical expertise, organisational and financial resources, and expertise and resources are not distributed equally across states. Still, there is a need for all states to participate in this dialogue. Investments in international law capacity building are thus to be encouraged.

The next part of the Report turns to the regulation of ransomware under international law, examining the application of international law to cyberspace, the types of disagreements on the content of the law, and the fora engaged in the law's clarification and development.

Part II.

How international law regulates ransomware

International law is highly relevant to ransomware operations. **While international law does not specifically prohibit ransomware operations, as such, many customary and treaty rules limit the freedom of states to engage in ransomware. Further, international law imposes positive obligations requiring states to take protective measures against the threats posed by ransomware operations.** At the same time, the precise scope of these rules is often disputed, which limits their impact on state conduct.

To understand international law's substantive rules, it is first necessary to engage with three threshold questions. This is done in the subsequent sections, which (1) clarify that international law **applies** to conduct carried out through ICTs, (2) identify **four levels of disagreement** about the content of international law, and (3) identify the **fora engaged in the clarification, specification and development of international law** relevant to the regulation of ransomware operations.

1. Applying international law to cyberspace

The conduct of ransomware operations *through ICTs* does not displace existing protections under international law. It is well-established that international law *applies* to conduct relying on ICTs.[32] This conclusion has been reached by two inter-governmental groups seeking to address the risks and ways of tackling contemporary cyber threats – the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security ('the OEWG') and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security ('the GGE'). Both groups have taken steps to clarify not only that international law *applies* to conduct in cyberspace, but also *how* international law applies. Despite baseline consensus, discussions held within the OEWG and GGE reveal a significant measure of disagreement.

2. How do states disagree about international law applied to cyberspace?

Disagreements over the application of international law to cyberspace operations, including ransomware, can be located at different levels. Understanding the type and level of disagreement provides a basis for meaningful engagement with that

disagreement. Four levels of disagreement have particular relevance in the context of cyberspace regulation.

First, states disagree on the existence of rules of general international law, irrespective of their applicability to cyberspace. This type of disagreement has become prominent in the discussions on the principles of sovereignty and Corfu Channel due diligence (discussed below). Thus, we read in a statement by the United States that '[i]n recent public statements on how international law applies in cyberspace, a few States have referenced the concept of "due diligence": that States have a general international law obligation to take steps to address activity emanating from their territory that is harmful to other States, and that such a general obligation applies more specifically, as a matter of international law, to cyber activities. The United States has not identified the State practice and *opinio juris* that would support a claim that due diligence currently constitutes a general obligation under international law.'[33] States taking this position will point out that, while some states have affirmed the existence of a general obligation of due diligence as a matter of customary international law, as outlined in the Corfu Channel judgment by the International Court of Justice, the existing practice does not constitute 'general practice accepted as law', as required for the formation of a rule of custom.[34] They will additionally point out that each tribunal award or court judgment affirming due diligence duties had been made in specific contexts – maritime navigation or environmental protection – suggesting that it is not a rule of general application. This level of disagreement can be unpacked and analysed through the rules on the formation of international law, that is, the methodology for the identification of customary rules and general principles of law, and the rules on the formation of treaties.

Second, states agree on the existence of general rules of international law yet dispute their extension to conduct carried out in cyberspace. In relation to obligations of due diligence under customary law, Israel said the following: 'we have to be careful in applying to the cyber domain rules that emerged in a different, distinct context. [...] However, we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching *opinio juris*, which would be indispensable for a customary rule of due diligence, or something similar to that, to form.'[35] Here, the objection relates not to the existence of the rule in general under customary international law – the claim is cyber-specific.

Third, states agree on the existence of rules of international law and their applicability to cyberspace yet dispute the elements of these rules. This is the most common form of disagreement. States have advanced divergent positions on the elements of the prohibitions of intervention and of the use of force, of the Corfu Channel principle and no-harm rule. To address this type of disagreement, it is necessary to engage with the principles governing the identification of customary law and treaty interpretation.

Fourth, states agree on the existence of rules, their application to cyberspace and their elements, yet disagree on the particular ways of discharging their obligations. This is particularly relevant in the context of positive obligations under international law. For instance, in considering protective measures under human rights law in the context of ransomware, some states may adopt legislation prohibiting ransom payments domestically, and others may seek to constrain ransomware in other ways, such as the

regulation of the cryptocurrency market. These types of disagreements can be addressed through the specification of obligations, an examination of the margin of appreciation conferred to states, and the other applicable obligations constraining or enabling their planned measures.

Types of disagreement

1. Disagreement on the existence of the right/ obligation under customary international law
2. Disagreement on the extension of an existing right/ obligation to cyberspace
3. Disagreement on the specification of the elements of an existing rule (in general or when applied to cyberspace)
4. Disagreement on the measures necessary to discharge particular obligations

3. Fora for the clarification, specification and development of international law in relation to cyberspace operations

As demonstrated in the previous section, disagreements on the content of international law, and in particular on its content applied to ICTs, continue to pervade international discussions. These disagreements, in turn, affect the constraining function of the law, as much of it may be seen as 'open to debate'. This is why recent years have seen vigorous efforts to clarify the application of international law to cyberspace.

Discussions on the interpretation and application of international law to operations conducted via ICTs, including ransomware operations, are taking place in inter-governmental settings. Beyond the OEWG and the GGE, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes is of particular relevance.[36]

Individual states have also taken the lead on specifying the content of international law through detailed national positions. The recent positions of Costa Rica,[37] the Netherlands,[38] Estonia,[39] Japan[40] and Canada,[41] among others, significantly contribute to the clarification of legal rules. The United Kingdom advanced its more fine-tuned understandings of the scope of the principles of sovereignty and non-intervention in the May 2022 speech of the then-Attorney General Rt Hon Suella Braverman QC MP entitled *International Law in Future Frontiers*.[42]

Non-state actors have made their own contributions to these discussions. Prominent examples are the **Oxford Process on International Law Protections in Cyberspace** and the **Tallinn Manual Process**, the former an academia-led initiative and the latter a flagship initiative of the NATO Cooperative Cyber Defence Centre of Excellence. Both initiatives operate on the basis of expert discussions geared towards the clarification of existing international law as it applies to cyberspace conduct and harms.[43] Private

sector companies have been active in supporting efforts to clarify existing standards and in shedding light on the technical dimension of cybersecurity and capacity building.

Through these intensifying exchanges on the content of international law, it becomes possible to identify pockets of agreement on the interpretation of legal rules. Equally, as noted in the previous section, it becomes easier to discern substantive divergences of opinion and key questions that have so far remain un- or under-addressed. The following sections seek to outline both areas of agreement and of continued contestation in the interpretation of legal rules. **The identification of the scope of international legal obligations plays a dual function: first, it tells the addressees of obligations what they must do or abstain from doing (communicative function); and second, it provides a basis for claiming and implementing responsibility for an internationally wrongful act, where a state has violated its obligations under international law (response function).**

The next part of the Report turns to the substantive rules that bind states in relation to ransomware operations. A wealth of obligations, positive and negative in character, require states to **abstain** from acts constituting or contributing to ransomware operations, and **to take measures** to prevent or minimise the ransomware threat. Given that the bulk of ransomware operations originate from non-state actors with either no links to a state, or with links that are insufficient to ground attribution to that state, the Report will first examine the obligations arising in the context of non-state actor activity and then turn to state threats.

Part III.

A system of international law obligations for assessing non-state and state ransomware threats

States are responsible for their own conduct that constitutes a breach of an international obligation.[44] Some obligations require the state to act, and thus a failure to act will breach international law. Other obligations require the state to abstain from certain forms of conduct, and the breach will manifest when the prohibited conduct is carried out. The conduct of private actors is not, as a general rule, attributed to the state. To provide a comprehensive overview of international law protections against ransomware, this Part examines the obligations of states both where ransomware operations can and cannot be attributed to them.

1. The non-state ransomware threat

A. Criminalisation obligations

Cybercrime has been at the forefront of state attention for decades. Domestic legislation and regional frameworks are the primary tools that have, to date, been used to tackle cyber criminality. Among others, the Economic Community of West African States adopted a directive tackling cybercrime,[45] Arab states established the Arab Convention on Combating Technology Offenses,[46] and the Council of Europe drew up the Convention on Cybercrime (also known as the Budapest Convention), making it the first international treaty tackling computer crime through a range of measures, including the harmonisation of national laws and international cooperation.

The Budapest Convention, to which the United Kingdom is a party, provides an important framework for the criminalisation of conduct, for investigative powers in relation to cybercrime and powers to secure electronic evidence, and for international co-operation. Parties to the Convention are members of the Cybercrime Convention Committee, which is a forum for discussion, collaboration, implementation assessment and interpretation of the Convention. The Convention was, in 2022, bolstered by a Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence. Through this Protocol, states can deepen cooperation on cross-border investigations of cybercrime. More recently, on 30 November 2022, the Cybercrime

Convention Committee of the Budapest Convention adopted a guidance note on aspects of ransomware covered by the Convention.[47]

While the **Budapest Convention** does not explicitly regulate ransomware operations, many of its substantive and procedural provisions address the ransomware threat. Under the Convention, **parties must adopt legislative and other measures 'to establish certain criminal offences under their domestic law, when committed intentionally and without right.'**[48] **Provisions of particular substantive significance are those on illegal access, data and system interference, misuse of devices, computer-related fraud.** Procedurally, the Convention and its second protocol provide **important avenues for cooperation**, such as **emergency mutual assistance and expedited disclosure of stored computer data in an emergency**. The three principles governing cooperation under the Convention are, as follows: international cooperation is to be provided among parties 'to the widest extent possible'; cooperation is to be extended not only to all criminal offences related to computer systems and data, but also to the collection of evidence in electronic form related to *any* criminal offence; the provisions of the Convention do not supersede any other international agreements, including agreements on mutual legal assistance and extradition. Importantly, the Budapest Convention, in its regulation of mutual legal assistance, provides for acceleration mechanisms to avoid the loss of critical evidence. Thus, states can make urgent requests for co-operation through expedited means of communications, and the requested parties must use expedited means to respond. States can also ask for expedited preservation of stored computer data. A network of 24/7 points of contact is also established through the Convention to ensure and facilitate immediate assistance.[49] More work is needed to determine precisely how ransomware operations fall within the ambit of substantive rules of the Budapest Convention, and how the provisions on enforcement and mutual assistance relate to the principle of sovereignty.

Since 2021, the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes has been convening meetings in New York in view of negotiating an international cybercrime treaty. The purpose of the treaty is to both criminalise certain forms of conduct and improve cooperation between states. While the negotiations are underway, many have approached this effort with caution, including the European Union.[50] An early draft submitted by the Russian Federation caused alarm in non-governmental organisations, prompting fears that the international cybercrime treaty could be used to stifle dissent.[51] Indeed, some states favour a broad approach to the criminalisation of both cyber-dependent (offences that can only be committed by ICTs) and cyber-enabled offences (traditional offences whose scale or reach is enhanced by the use of technologies), while others fear that a broad approach to cyber-enabled offences could lead to abuse. **Great care will be needed in negotiating an instrument that strikes an appropriate balance between**

Great care will be needed in negotiating an instrument that strikes an appropriate balance between the protection of human rights, sovereignty interests, and the need to curb and prevent cyber criminality.

the protection of human rights, sovereignty interests, and the need to curb and prevent cyber criminality. The concluding session of the UN Ad Hoc Committee is scheduled for 29 January - 9 February 2024.[52]

In addition to existing and currently negotiated instruments designed to tackle cybercrime, sectoral treaty regimes contain criminalisation obligations relevant to ransomware. For instance, under the **International Convention for the Suppression of the Financing of Terrorism**, states parties must establish as criminal offences under their domestic law the provision or collection of funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out acts of terrorism. States parties must also ensure that these acts of funding or collection of funds are punishable by appropriate penalties which take into account the grave nature of the offences.[53] States must also comply with sanctions regimes imposed in accordance with the Charter of the United Nations.

B. Positive obligations under international human rights law

International human rights law is comprised of international[54] and regional[55] treaty regimes and customary rules geared towards the protection of individual interests from and by states. The addressee of obligations is the state, the object of protection the individual. The precise scope of a state's obligations depends on the treaty regimes it is bound by, and on the content of customary human rights law.

Quite clearly, **ransomware operations can implicate the rights of individuals arising under a range of rights, including the rights to life, health, privacy and property**. By way of example, a ransomware operation disrupting the provision of emergency healthcare can affect the enjoyment of the rights to life and health, and a ransomware operation that accesses private data can affect privacy.

International human rights law binds states to both negative and positive obligations, which they must ensure to those individuals under their jurisdiction. **Negative obligations require states to abstain from certain forms of conduct while positive obligations require states to take positive steps towards a given goal.** Positive duties obligate states to take certain steps to safeguard rights-holders from harm, including when such harm originates from non-state actors. This latter point is of particular relevance to ransomware operations, since many such operations are carried out by private criminal groups without connections to a state. The central question is how far these positive duties reach.

International human rights law binds states to both negative and positive obligations, which they must ensure to those individuals under their jurisdiction.

Negative obligations require states to abstain from certain forms of conduct while positive obligations require states to take positive steps towards a given goal.

In the context of the right to life, the Human Rights Committee has affirmed that '**States parties are thus under a due diligence obligation to take reasonable, positive measures that do not impose disproportionate burdens on them in response to reasonably foreseeable threats to life originating from private persons and entities whose conduct is not attributable to the State.**'[56] Translating this duty to the context of ransomware, the Oxford Statement on Ransomware Operations clarifies that

> States must take measures to protect the human rights of individuals within their jurisdiction from harmful ransomware operations, including when such operations are carried out by other states and non-state actors. To discharge this obligation, states may, among other measures, prohibit ransomware by law, take feasible steps to stop ransomware operations, mitigate their effects, investigate and punish those responsible, as well as prevent and suppress ransom payments to the extent possible.

Positive obligations under international human rights law require states to take action in the face of reasonably foreseeable threats. Importantly, this regime provides the following:

- **Flexibility** in the ways of discharging particular positive obligations.
- **Concrete suggestions for managing risk**. For instance, the Human Rights Committee opined that states parties should 'develop, when necessary, *contingency plans and disaster management plans* designed to increase preparedness and address natural and manmade disasters that may adversely affect enjoyment of the right to life, such as hurricanes, tsunamis, earthquakes, radioactive accidents and *massive cyberattacks resulting in disruption of essential services*.'[57] Some have argued that the ransomware threat requires bolstered obligations to increase transparency in the reporting of ransomware incidents, defensive capabilities and payments.[58]
- **Tailored standards based on the type of activity in question**. The European Court of Human Rights has developed a rich jurisprudence on positive obligations arising in relation to **dangerous activities**, such as industrial activities. For such activities, special emphasis has been placed on regulations governing their 'licensing, setting up, operation, security and supervision', as well as on practical measures for minimising risk.[59] In such cases, the Court has also emphasised the public's right to information. Given the rise of cyber threats, and in particular the concerning trend of operations against critical infrastructure, including through ransomware, a robust standard for positive obligations akin to that applicable to dangerous activities would be in order.
- **A framework for balancing interests**. In cases where protective measures would interfere with other human rights, these measures must comply with the applicable legal requirements of legitimate purpose, legality, necessity, proportionality and non-discrimination. This framework may become particularly important in considering the regulation of ransom payments. Although there is

emerging domestic practice for prohibiting certain entities from complying with ransom demands,[60] states are still seeking to identify the optimal approach to this question.[61] In that identification process, the tests required for compliance with human rights law must play a prominent role.

- **Review mechanisms.** Most human rights treaty instruments establish supervisory bodies. The availability of review mechanisms is a particular advantage of the human rights framework, as it allows a continuous conversation on the application of human rights and the scope of state obligations against the background of evolving threats.

- **A possibility for anchoring inter-state cooperation in legal duties.** Because of the interconnectedness of threats, and the location of servers operating critical infrastructure of states on the territory of other states, obligations arising under international human rights law may require the establishment of channels of communication at the inter-state level. The digital dependencies of infrastructure create systemic risks[62] that can only be addressed through common collaborative frameworks. In many ways, such cooperation based on international law would align with the efforts taken at the UN to establish national points of contact managed through a common Directory.

C. The Corfu Channel and no-harm rules

Under a range of treaty-based and customary international law rules, states are bound to exercise due diligence in the protection of certain interests from harm. Such obligations exist in environmental law, human rights law and humanitarian law, among others. While some contrary views remain, many states and scholars affirm the existence of two obligations under customary international law containing a due diligence standard that could be particularly relevant to cyberspace. They are the Corfu Channel rule and the no-harm rule. Importantly, these rules would require states to take positive measures to address threats originating from non-state actors.

Under a range of treaty-based and customary international law rules, states are bound to exercise due diligence in the protection of certain interests from harm.

The Corfu Channel rule posits an obligation for states not to allow knowingly their territory to be used for acts contrary to the rights of other states. Acknowledged by the International Court of Justice in its *Corfu Channel* Judgment[63] – and carrying its name –

this rule has an important regulatory potential in the field of ransomware operations. As with positive obligations under human rights law, states would not be responsible *for* the act contrary to the right of other states performed from their territory. Rather, **they would be responsible for their own omissions in relation to a harmful act committed by others,** subject to knowledge and feasibility requirements. According to some, this rule would only cover the halting of ongoing harmful acts. According to others, it extends to a full spectrum from prevention through halting and mitigating to redress. This rule opens a door to claims of violation for states that have become safe havens for ransomware criminal groups. Importantly, the Corfu Channel rule does not require states to achieve a particular result, such as the prevention of all harmful operations. Its scope depends on the capacity of the state that has to exercise due diligence. This flexibility makes it difficult to identify the exact scope of a particular state's obligations in the abstract.

The no-harm rule obligates states to prevent, stop, and redress significant transboundary harm to persons, property or the environment. This obligation exists irrespective of attribution of this conduct to a state, and it covers activities not prohibited under international law. The meaning of 'significant harm' is key to unlocking the regulatory potential of this rule. If a state fails to exercise due diligence under this rule and significant harm occurs as a result, it is liable to pay compensation. It is only if the state fails to compensate that it will incur state responsibility under the no-harm rule.[64] While the principle enjoyed particular significance in debates about environmental harm, it need not be limited to this context.[65] However, states relying on it in the context of ransomware operations will have to demonstrate the existence of **significant** transboundary harm.

2. The state-based ransomware threat

Although the majority of ransomware operations find their origin in the conduct of non-state criminal groups, states are also involved in ransomware themselves. States can be involved in two main ways. First, states can carry out ransomware operations through their own organs or entities exercising elements of governmental authority. Second, states may be implicated in a particular way in conduct carried out by private actors, e.g. because they provide instructions, direction or control, or because they acknowledge and adopt the private conduct as their own. In both scenarios, the state's involvement means that the ransomware operation is **attributed** to the state.

Attribution of conduct to a state

Attribution in the legal sense is distinct from both the technical attribution to a responsible cyber actor and the political attribution to a given state, organisation or individual.[66] This section deals with attribution in the legal sense.

Legal attribution describes the operation of attaching a given conduct, by an individual or a group, to a state. As a legal entity, a 'state' cannot act *itself,* but is responsible for conduct that is attributed to it.[67]

The customary law of state responsibility identifies various grounds for attribution.[68] The most obvious way in which states act is through their organs. **State organs** can be either entities officially designated as such (*de jure* organs) or entities that, as a matter of fact, are completely dependent on the state (*de facto* organs). In the latter case, even if a state does not formally recognise an entity as its organ, it will bear responsibility for its conduct where such entity has no autonomy vis-à-vis the state. This precludes the possibility of circumventing state responsibility for entities that are, in fact, under a state's full and strict control. Further, **a state can empower an entity by law to exercise elements of the governmental authority**. For both state organs and entities exercising elements of governmental authority, the state bears responsibility even for acts that exceed authority or contravene instructions.[69]

Importantly for the cyber context, the conduct of private actors **acting on the instructions of, or under the direction or control of a state** is also attributable to that state. The jurisprudence of the International Court of Justice in the *Nicaragua* and *Bosnian Genocide* cases has set a consistently high bar for the test of control, namely effective control over *specific* operations. This is important, as the cyber context has shown that states, even where they are linked to hacker groups, often will not control their specific operations.[70] A good example is the relationship between Russia and the ransomware hacker group Conti. 60.000 chat messages and files leaked at the start of 2022 revealed close ties between the group and the Russian Federal Security Service (FSB), including communication between the entities and Conti's awareness of FSB operations.[71] While Conti's activities align with Kremlin-defined Russian national interests, there is little to suggest that the group is either completely dependent on the state or that Russia is controlling specific hacking operations, making attribution of its conduct to Russia difficult. Some states have sought to specify the application of the 'effective control' test to cyberspace. According to Germany, '[w]hile a sufficient degree or intensity of such control is necessary, the State is not required to have detailed insight into or influence over all particulars, especially those of a technical nature, of the cyber operation.'[72] Further fleshing out of the levers of control and influence relevant for attribution should be a priority for states.

Finally, outside instances of instruction, direction or control, conduct carried out by private groups can be attributed to a state through ***ex post facto* acknowledgment and adoption**. This possibility was confirmed by the International Court of Justice in the *Tehran Hostages* case.

The implications of attribution

Attribution in cyberspace raises complex questions. To begin with, attribution is dependent on the availability of information on the origin of a particular operation. This,

in turn, brings to the fore questions of disparate capacities among state actors. Additionally, attribution is a politically fraught question, the policy implications of which may disincentivise states from making public statements attributing conduct. Even if a state does decide to attribute conduct to another state, some have argued that the attributing state must further disclose the evidence substantiating its attribution claim.[73] As credible claims of attribution may require states to disclose their detection and analytical capacities or affect the security of sources, state often decide against public attribution.

Additionally, attribution to a state may impact insurance coverage. Amidst rising pressures on the insurance industry, Lloyds announced, in the summer of 2022, the exclusion of coverage in cases of state-sponsored cyber operations.[74] These rising pressures are in large part due to the rise in ransomware, and the consequent rise in ransomware insurance claims. In order to determine whether a particular operation qualifies as a 'state-sponsored cyber operation' (and is therefore not covered), it is necessary to identify its source or origin. In practice, insurers themselves will have to determine whether a particular operation has been 'state-sponsored'. It is unclear whether their analysis will be grounded in notions of international law. This may, in turn, create a disparity between the legal tests for attribution in international law and contractual terms that rely on language similar to the international standards. It is crucial to have clarity over the standard applied by the insurance sector.

Attribution of conduct is an essential element of establishing another state's responsibility. Under international law, such responsibility arises from attributable conduct that violates a state's obligations under rules of international law. Current debates reflect a broad measure of agreement on which rules are of particular significance, namely the principle of sovereignty, the prohibition of intervention, international and regional human rights law, the prohibition against the threat and use of force, the Corfu Channel and no-harm rules. Because the previous section examined positive obligations under international human rights law, the Corfu Channel and no-harm principles, this section will not review them anew. Suffice to say that these positive obligations can be triggered regardless of the source of harm – state or non-state.

The following sections trace the elements of relevant international obligations and apply them to ransomware operations.

A. The principle of sovereignty

Sovereignty is an organising principle of international law, which finds a concrete manifestation in the sovereign equality of states, the rules on jurisdiction, non-intervention and the use of force. **Recent years have seen a wealth of opinions, both state and academic, suggesting that sovereignty is not only a principle, but a self-standing rule of international law with its own normative content**. Canada's April 2022 national position on the application of international law to cyberspace dedicates twelve paragraphs to the contours of sovereignty as a rule.[75] In contrast, the United Kingdom considers there to be insufficient evidence in state practice and *opinio juris* – the constitutive elements of customary international law – to extrapolate a rule of sovereignty from the principle.[76] The debate persists.

Those advocating for a self-standing rule of sovereignty typically identify two forms of violations. First, where an attributable cyber operation causes harmful effects on the territory of another state; and second, where it interferes with or usurps inherently governmental functions of another state (even where no territorial effects are caused). What an inherently governmental function is, is typically explained through illustrations, rather than a definition, which range from healthcare and elections to crisis management and national security.[77] The Tallinn Manual, and specifically the experts convening the Tallinn Manual Process, have been particularly active in advocating for the rule in this dual-track form.

With ransomware, depending on the effects and target of the operation, the proposed self-standing rule becomes particularly significant. For instance, ransomware operations can usurp the performance of healthcare functions, including pandemic responses. Similarly, by locking systems and data, they have the capacity to cause tangible harms, including injury and death. This suggests that a rule of sovereignty would circumvent many of the difficulties over defining the element of coercion in the prohibition of intervention (discussed in the following section), making ransomware (if attributed to another state) actionable as a breach of sovereignty. However, even states and scholars who consider the principle of sovereignty to qualify as a self-standing rule have yet to agree on the precise threshold for its application.

B. The prohibition of intervention

International law contains a binding rule prohibiting coercive intervention in another state's *domaine réservé*.[78] In the *Nicaragua* Merits Judgment, the International Court of Justice found that this rule is well-established in customary international law, and that it prohibits interferences involving 'methods of coercion' oriented towards the internal or external affairs of a state.[79] 'A prohibited intervention must', according to the Court, 'be one bearing on matters in which each State is permitted, by the principle of State

sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy.'[80]

While the rule is well-established under customary international law, its contours remain contested. This, in turn, affects its effectiveness, including its deterrent effect. For instance, **what is a method of coercion**? Would a state have to act with an *intention* to coerce, or can certain methods be considered objectively coercive without inquiring into the intentions of the perpetrator? Interpretations vary. The need for subjective intent seems implicit in the position of the Netherlands, which defines intervention as 'interference in the internal or external affairs of another state *with a view to* employing coercion against that state.'[81] In contrast, the position of the United Kingdom, as explained in the *International Law in Future Frontiers* speech, seems open to accommodating a wider interpretation. It provides that 'an intervention in the affairs of another State will be unlawful if it is forcible, dictatorial, *or otherwise coercive*, depriving a State of its freedom of control over matters which it is permitted to decide freely by the principle of State sovereignty.'[82]

International law contains a binding rule prohibiting coercive intervention in another state's domaine réservé.

Applied to the present context, **ransomware operations are by definition coercive. However, they do not necessarily 'bea[r] on matters in which each State is permitted … to decide freely'**. Notably, they can be coercive towards the individual or entity victim of the operation without having any effect on or demands towards state choices. The extent to which the prohibition against intervention applies to ransomware operations largely depends on the interpretation of the element of coercion in its relationship to a state's *domaine réservé*. This, in addition to the problems of attribution outlined above, often makes it difficult to qualify ransomware operations as prohibited interventions.

C. International human rights law

As noted previously, international human rights law is an area of international law comprised of international[83] and regional[84] treaty regimes and customary rules for the protection of individual interests. International human rights law imposes upon states negative and positive obligations. Negative obligations require states to abstain from certain forms of conduct while positive obligations require states to take positive steps towards a given goal. Positive duties obligate states to take certain steps to safeguard rights-holders from harm, including when such harm originates from other states.

Negative obligations can arise under a range of rights, including the right to life, health, privacy, education. For instance, according to the Human Rights Committee, **states must abstain from acts that can foreseeably and unjustifiably interfere with the right to life**.[85] Thus, ransomware operations mounted by, controlled, or otherwise

acknowledged or endorsed by a state that implicate the provision of healthcare can lead to responsibility under international human rights law.

International human rights law applies to state conduct vis-à-vis individuals under the state's jurisdiction. The meaning of jurisdiction has an accepted core: international human rights apply to a state's conduct on its own territory. By contrast, it is **disputed to what extent human rights apply to the extraterritorial conduct** of a state. While human rights regimes differ, as a general trend, human rights case-law indicates that states are required to observe human rights extraterritorially where they exercise control over persons or spaces. As many state-driven ransomware operations are cross-border in nature, the interpretation of extraterritorial jurisdiction will greatly affect the scope of protection that can be claimed under human rights law.

Importantly, human rights treaties often contain provisions on the establishment of review mechanisms – committees, commissions, courts – that can both clarify the scope of applicable human rights and operationalise responsibility.

D. The prohibition of the threat and use of force

Under art. 2(4) of the Charter of the United Nations, **states must refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations**. This prohibition exists under both treaty and customary law. Despite the centrality of the prohibition in the international system and its frequent description as a peremptory rule of international law, its scope remains disputed in a number of ways. For instance, it is still debated whether the prohibition covers the objective projection of force across state boundaries or requires an intent to use force against another state.[86] Further, states and scholars have for many years disagreed over whether the notion of 'force' is subject to a *de minimis* threshold, thus excluding 'minor' forcible actions.[87] More recently, **the use of ICTs in inter-state operations has added another layer of complexity to the question of defining the term 'force'**.

When it was drafted, the Charter prohibition clearly sought to constrain *armed* force, rather than economic or political force.[88] What is unclear, however, is what armed force looks like in the digital space. Some, including the experts of the Tallinn Manual process, have sought to identify **factors that can assist determinations on the existence of a use of force. These factors include severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality**.[89] Some states are open to the possibility that actions not producing any physical effects could amount to 'force', France and the Netherlands being prime examples. Without physical effects, the French position requires a consideration of 'the circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not), the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target.'[90] Depending on which factors states emphasise, ransomware operations will be more or less likely to

reach the threshold of a use of force. While their effects can be severe, they will not necessarily manifest in an immediate or direct way.[91]

Recent national positions have also sought to move the interpretation of 'force' to certain forms of economic or political harm. Thus, according to the Netherlands, 'at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force',[92] and 'Denmark considers that it generally cannot be ruled out that acts of economic or political coercion can fall within the purview of Article 2(4) of the UN Charter if, for example, a cyber operation resulting in the malfunctioning of a State's financial system leads to significant economic damage.'[93]

Although most scholarly and state attention has been devoted to the prohibition of the use of force, its counterpart, the prohibition of threats of force, deserves particular attention.[94] Depending on the circumstances, an access breach into the victim's system may not constitute a use of force but indicate the existence of a threat of force in the meaning of a signalled intention to use force at a future point, unless a demand is met.

Difficulties over insurance coverage arise with common 'act of war' exclusion clauses. Recent lawsuits between insurers and clients seeking to cover the costs associated with the NotPetya malware are instructive in this regard. Insurers made the claim that NotPetya had constituted 'hostile or warlike action',[95] while a New Jersey appellate court ruled, in connection to a USD 1.4B claim made by Merck, that the *NotPetya* attack 'is not sufficiently linked to a military action or objective as it was a non-military cyberattack against an accounting software provider'.[96] An appeal by the insurers will be heard by the New Jersey Supreme Court.[97]

Part IV.

Responding to breaches of international law

As shown in the previous sections, international law contains a wide range of rules that regulate ransomware activities. Some of these rules require states to take positive measures to address threats of whatever origin. In some instances (e.g. with respect to duties to legislate), the positive measures require the establishment of domestic regulatory frameworks. Other positive measures are technical and organisational, and may require states to set up cybersecurity defence requirements, establish computer emergency response teams, or organise education campaigns on cyber hygiene, among others. Positive obligations build domestic resilience, which is key to preventing and mitigating cyber harms. Beyond positive obligations, international law requires states to abstain from certain forms of conduct that impair rights of individuals or of other states. Positive and negative obligations, viewed together, comprise a system of rules requiring states to **respect** the interests of others and to **protect** from cyber harms. In many instances, ransomware activities, even where they are carried out by criminal groups, will be facilitated by a state's violation of its obligations under international law. Other states can respond against such breaches, both in response to states that themselves engage in ransomware operations, and against states that allow criminals to operate from areas under their jurisdiction or fail to take sufficient measures to protect from cyber harms.

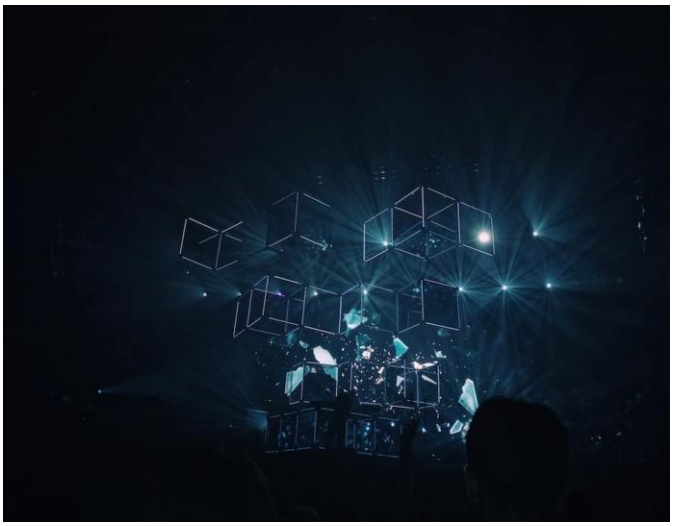
How states respond to breaches of these obligations is dependent on the type of breach, its context, the relationship with the wrongdoing state, the respective capacities of the states involved, and the available mechanisms for review. Depending on these considerations, some breaches may best be addressed through increased dialogue and collaboration, others can call for a more robust response that involves forms of lawful pressure aimed at inducing the wrongdoing state to cease its wrongful conduct or redress its consequences. Fundamentally, **international law leaves states significant leeway in fashioning their responses to unlawful conduct.** At a very general level, three types of responses can be distinguished, which in practice often go hand in hand.

International law leaves states significant leeway in fashioning their responses to unlawful conduct.

1. Non-coercive responses

In some cases, the best way to ensure further compliance is to engage in dialogue with the wrongdoing state. This will especially be the case where the wrongdoing state has failed to prevent or stop ransomware operations committed by private actors, and may benefit from assistance in building domestic capacity to deal with future threats.

Confidence- and capacity-building are two other forms of assistance that can help counter ransomware threats. Confidence-building measures comprise 'transparency, cooperative and stability measures' that can contribute to 'preventing conflicts, avoiding misperception and misunderstandings' and reducing tensions.[98] Capacity-building is based on the understanding that the security of the entire international community in the face of cyber threats depends on the capacity of each state to prepare and respond. Capacity-building is thus geared towards the development of skills, policies and institutions that can ensure resilience and meaningful participation in international cooperation. **Given the discrepancies in states' technological development, and the crucial role of domestic cyber resilience against attacks by private actors, capacity-building remains central to mitigating ransomware threats**.



2. Protests and formal complaints

Protests are a routine form of responding against another state's breaches of international law. For the reasons mentioned above, states may at times be reluctant formally to attribute particular attacks to another state. However, where the evidence is clear, **public protests – the 'calling out' of a violation – are an important part of an effective response**. The forms of such protests vary depending on the type of breach in question. Government-to-government responses remain common. Treaty regimes often establish **mechanisms to address disputes within institutional settings**. This is particularly relevant in the context of human rights treaties, which have established a wide range of bodies (committees, regional courts, etc.) that can scrutinise state conduct against the benchmarks of human rights obligations. For instance, the Universal Periodic Review, a state-driven process within the auspices of the Human Rights Council, involves a review of the human rights records of all UN Member States. Such mechanisms can also have a deterrent effect, as the need to justify state conduct may lead states to better implementation of their obligations. So far, states have been relatively hesitant to rely on these institutional mechanisms. Experience with other fields of international law indicates that human rights mechanisms can **provide platforms for naming and shaming wrongdoing states**.

3. Coercive responses

Beyond collaborative responses and protests, states may decide to respond coercively against states violating their obligations. International law leaves significant

room for such coercive responses which are intended to put pressure on wrongdoing states. Unfriendly, yet lawful measures – referred to, in international law's parlance, as 'retorsions' – are an obvious first step.[99] Especially where states are integrated into dense cooperative relationships or depend on outside support, the withdrawal of benefits granted to them can be effective: typical examples include the suspension or withdrawal of aid programmes, trade restrictions or diplomatic snubs (up to the severance of diplomatic relations). In the cyber-sector, states can respond to breaches by, for example, sending warnings to cyber operatives involved in the illegal operations. As long as these measures are merely 'unfriendly', but do not violate international obligations, the responding state can take such measures at will.

Beyond this, international law allows for the taking of measures that can have a higher impact, and that therefore come with their own distinctive advantages.

International law as set out in the preceding sections outlines the contours of prohibited and required behaviour; it equally provides a range of mechanisms for the invocation of responsibility and responding to violations. How and where particular violations may be invoked depends, to a large extent, on the specific rule in question, as well as on the existence of procedures established by particular treaty frameworks. As a matter of customary international law, states have a legal right to invoke the responsibility of another state either when they are injured by the internationally wrongful act (notably if a ransomware operation affects their territory, public services or persons under their jurisdiction) or exceptionally where the *nature* of the breached obligation envisions invocation by non-injured states (for obligations *erga omnes*, that is, obligations owed to the international community as a whole, and obligations *erga omnes partes*, that is, obligations established for the protection of a collective interest of the group).[100] Invocation will typically entail the bringing of a claim in front of a formal mechanism, such as a court or a tribunal.

Beyond this, states can take decentralised enforcement measures, referred to as countermeasures. **Countermeasures are measures that, but for the internationally wrongful act of the responsible state, would be contrary to the international obligations of the state taking the measures.** Their nature as a response action to a prior illegality is what *precludes their wrongfulness*. **The purpose of countermeasures must be to induce a change in behaviour in the responsible state**, to bring it back into compliance with its international obligations. Countermeasures must be proportionate to the injury suffered and are subject to a list of procedural and substantive conditions. In the context of ransomware, states can take countermeasures not only against states engaged in the commission of ransomware, but also towards those that harbour criminal groups in breach of the Corfu Channel rule and positive obligations under international human rights law.

While countermeasures permit potentially 'robust' responses against states engaged in ransomware operations, they presuppose that such ransomware attacks have actually violated international law. In this respect, the ongoing debate about the precise scope of certain rules of international law (noted in the preceding sections of this Report) can spill over into debates about countermeasures. For instance, it is unclear whether the Corfu Channel due diligence obligation, if accepted to exist under

customary international law, requires the causation of **a particular harm** as an element necessary for the existence of a breach, or that harm is simply a condition for legal standing in respect of invoking responsibility. If harm is *not* required and one accepts the broad 'preventive' scope of the rule, this would mean that states can invoke countermeasures for the mere failure of a state to take legislative, organisational, technical and other measures necessary to protect against the risk of acts contrary to the rights of other states. Thus, ambiguity in the primary obligations can introduce uncertainty in the legality of enforcement through countermeasures.

One of the thorniest questions regarding countermeasures is whether non-injured states can rely on this circumstance precluding wrongfulness, either at the request of an injured state or on an *erga omnes* or *erga omnes partes* basis. While some states, including Estonia,[101] seem open to the possibility of non-injured states to take action under the countermeasures heading, it is far from clear that there is sufficient state practice and *opinio juris* to allow for this possibility, be it under general international law or through a cyber-specific evolution of custom.[102]

Beyond countermeasures, states can seek to shield protected interests from ransomware-related harms by resorting to another circumstance precluding wrongfulness – **necessity**. Under the doctrine of necessity, the wrongfulness of a breach of an international obligation can be precluded where the conduct in violation is the only way for the State to safeguard an essential interest against a grave and imminent peril and it does not seriously impair an essential interest of the state or states towards which the obligation exists, or of the international community as a whole.[103] While the ground of necessity has been approached with caution in international jurisprudence, due to its propensity for abuse, it may offer viable options in relation to cyberspace harms. This is because, unlike countermeasures, the act undertaken in conditions of necessity need not respond to a prior unlawful act of another state. This thus circumvents difficult questions around both attribution and the specification of primary obligations.

Finally, when the prior wrong amounts to an armed attack, states are entitled to use force to defend against that attack. Self-defence is an exception to the prohibition of the use of force allowing a state or group of states to use defensive force against an attacker. **As it presupposes an armed attack, self-defence will hardly ever be available as a response to ransomware attacks**. Nonetheless, the particular risks of cyberspace have prompted a number of states to argue in favour of pre-emptive measures to tackle cybersecurity threats. The 2018 United States Department of Defense Cyber Strategy adopts a 'defend forward' approach, allowing agencies 'to disrupt malicious cyber activity at its source, including activity that falls below the level of armed conflict.'[104] The goal is to stop threats before they reach their targets.[105] On 11 December 2022, it was reported that Japan is considering revisions to its National Security Strategy to allow 'monitoring of potential attackers and hacking their systems as soon as signs of a potential risk are established.'[106] If states take a narrow approach to the non-intervention rule and deny the existence of a sovereignty rule, or again, interpret this rule restrictively, it could be argued that such operations do not violate international law to begin with. Thus, they would fall within the confines of acts of retorsion. If, however, one takes a broader approach to the underlying primary rules, the 'defend forward' acts

may constitute breaches, thus needing a circumstance precluding their wrongfulness. And, if these operations are based on acts that could qualify as a use of force, their legality would depend on the availability of a self-defence justification. The better interpretation based on the rules of treaty interpretation is that self-defence, as the only justification for the use of force except Security Council authorisation, is triggered by the actual occurrence of an armed attack, not its *potential* occurrence.[107]

Similarly, countermeasures are contingent on the existence of an internationally wrongful act. Unless a state can demonstrate that the threat of harm is itself a breach of an international obligation, pre-emptive measures that breach a state's own obligations would not be covered by this circumstance precluding wrongfulness. Of course, state practice and *opinio juris* can lead to the development of the customary rule with new content. For now, however, the 'defend forward' approaches seem to appeal to a small group of states.

Ultimately, the best way of countering the threat of ransomware originating from both states and non-state entities is to ensure collaboration between states and other stakeholders, and to create the conditions for capacity-building and confidence-building to secure the resilience of networks and organisations. International law can provide a basis for such collaboration through its positive obligations under treaty and customary law, and, where collaboration fails, provide a basis for the taking of measures that can induce wrongdoers into compliance.

The best way of countering the threat of ransomware originating from both states and non-state entities is to ensure collaboration between states and other stakeholders, and to create the conditions for capacity-building and confidence-building to secure the resilience of networks and organisations.

Part V.

Conclusion and recommendations

This Report seeks to provide a toolkit for thinking about the threat of ransomware through the prism of international law. It offers an overview of the advantages of grounding calls for responsible behaviour in the language of international law. It further investigates the applicability of international law to operations conducted via ICTs, and examines the different layers of disagreements that exist on the content of international law. By locating these disagreements, the Report offers a guide to the methodology of navigating the different claims made by states and other stakeholders. In its substantive part, the Report identifies the international law rules most relevant to the regulation of ransomware operations. In its final part, it analyses the response options available to states.

Controversies remain over the elements of existing rights and obligations, and the need for additional rules to meet today's threats. In this process of developing and making international law, states remain central actors. In using their influence, states must be mindful of operational realities and strategic in their choices. When states advance particular interpretations of international law, they signal not only what they consider *others* should do or abstain from doing, but also what *they* are willing to abide by. This is why the approach to particular rules of international law and to the development of this legal framework more generally must be considered with great care.

In light of the foregoing, we make the following seven recommendations for operationalising international law protections in combating ransomware:

1. States must demonstrate a clear commitment to international law as a vehicle for countering the ransomware threat.
2. Given the interpretative controversies over the existence and scope of international law rights and obligations, states should engage in the further specification of international law, including through the publication of national positions on the application of international law to the use of information and communications technologies in general, and to ransomware operations in particular.
3. More focus is needed on positive obligations under international law, including on practical measures for the implementation of such positive obligations. For instance, states should consider the need for introducing reporting and other transparency obligations for ransomware incidents, regulation of ransom payments, cybersecurity defence requirements for at the very least entities responsible for critical national infrastructure, and crafting of cyber education campaigns. Any measure taken by the state must be in compliance with its human rights obligations, including the right to privacy.

4. In crafting domestic resilience measures, states should hold meaningful consultations with all relevant stakeholders.
5. Given the ransomware risks faced by public and private entities, governments should consider the establishment of public-private partnerships to assist victim entities in their recovery from ransomware incidents.
6. In responding to breaches, states should consider the spectrum of response options and avoid escalation.
7. A main vector for ransomware-related cyber harm is the lack of domestic expertise, knowledge and technical defence capacities. States should thus cooperate to build resilience, including through capacity-building efforts.

About the authors

Tsvetelina van Benthem is a post-doctoral researcher in International Law at the Oxford Institute for Ethics, Law and Armed Conflict and senior legal adviser at The Reckoning Project.

Christian J. Tams is Professor of International Law at the University of Glasgow, where he directs the Glasgow Centre for International Law & Security, and a Professor of International Law and Dispute Resolution at Leuphana University Lüneburg.

Scottish Council on Global Affairs
c/o Sir Alexander Stone building
University of Glasgow
Glasgow, G12 8QQ, Scotland, UK
john@scga.scot I scga.scot I @scga_scot

Endnotes

[1] Gordon Corera, 'Irish health cyber-attack could have been even worse, report says' (BBC News, 10 December 2021), available at: https://www.bbc.co.uk/news/technology-59612917.
[2] PwC, Conti cyber attack on the HSE: Independent Post Incident Review, 3 December 2021, available at: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf.
[3] Matt Burgess, 'The Untold Story of a Crippling Ransomware Attack' (WIRED, 30 January 2023), available at: https://www.wired.co.uk/article/ransomware-attack-recovery-hackney.
[4] Phil Muncaster, 'City of London on High Alert After Ransomware Attack' (InfoSecurity, 2 February 2023), available at: https://www.infosecurity-magazine.com/news/city-of-london-high-alert/.
[5] UK Finance, 'The Rise in Ransomware and Growing Government Concern' Banking and Finance Sector Position, May 2022.
[6] Ransomware Task Force, 'Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force', 2021.
[7] INTERPOL, 2022 INTERPOL Global Crime Trend Summary Report, October 2022, p. 6.
[8] Dan Milmo, 'NHS ransomware attack: what happened and how bad is it?' (The Guardian, 11 August 2022), available at: https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it.
[9] Jonathan Reed, 'Costa Rica State of Emergency Declared After Ransomware Attacks' (Security Intelligence, 16 November 2022), available at: https://securityintelligence.com/news/costa-rica-state-emergency-ransomware/.
[10] Cyber Management Alliance, 5 Major Ransomware Attacks of 2022, 15 June 2022, available at: https://www.cm-alliance.com/cybersecurity-blog/5-major-ransomware-attacks-of-2022.
[11] Sebastian Skelton, 'UK suffers third highest number of ransomware attacks globally' (Computer Weekly, 28 September 2022), available at: https://www.computerweekly.com/news/252525466/UK-suffers-third-highest-number-of-ransomware-attacks-globally.
[12] National Cyber Security Centre, A guide to ransomware, available at: https://www.ncsc.gov.uk/ransomware/home.
[13] The Oxford Statement on Ransomware Operations, available at: https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-ransomware-operations/.
[14] Microsoft Digital Defense Report 2022, pp. 9 – 10.
[15] Lance Whitney, 'The most dangerous and destructive ransomware groups of 2022' (Tech Republic, 25 October 2022), available at: https://www.techrepublic.com/article/most-dangerous-ransomware-groups/.
[16] Sophie Bushwick, 'FBI Takes Down Hive Criminal Ransomware Group' (Scientific American, 31 January 2023), available at: https://www.scientificamerican.com/article/fbi-takes-down-hive-criminal-ransomware-group1/.
[17] Tom Burt, 'Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression', Microsoft, 4 November 2022, available at:

https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/.

[18] The White House, International Counter Ransomware Initiative 2022 Joint Statement, 1 November 2022, available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/.

[19] G7 Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector (October 2022, available at: https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2022-G7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector.en.pdf) and G7 Fundamental Elements of Ransomware Resilience for the Financial Sector (October 2022, available here - https://www.mof.go.jp/english/policy/international_policy/convention/g7/20221021_1.pdf).

[20] UK HM Government, National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

[21] NCSC Annual Review 2022 page, available at: https://www.ncsc.gov.uk/collection/annual-review-2022/resilience/ransomware.

[22] For instance, see the NCSC Guide to ransomware, available at: https://www.ncsc.gov.uk/ransomware/home.

[23] For more information on GovAssure, visit https://www.security.gov.uk/guidance/govassure/.

[24] Allianz Global Corporate & Specialty SE, 'Cyber: The changing threat landscape: Risk trends, responses and the outlook for insurance', 2022.

[25] Lloyds, State backed cyber-attack exclusions, Market Bulletin Ref: Y5381, 16 August 2022.

[26] For the Statement, see here: The Oxford Statement on Ransomware Operations, available at: https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-ransomware-operations/. For the Oxford Process more generally, visit this page: https://www.elac.ox.ac.uk/the-oxford-process/.

[27] Jamie MacColl, James Sullivan, Jason R C Nurse, Sarah Turner, Gareth Mott, Edward Cartwright and Anna Cartwright, 'Cyber insurance and the ransomware challenge' RUSI Occasional Paper, July 2023.

[28] ILC, Articles on State Responsibility, arts. 42 and 48.

[29] id, arts. 30 and 31.

[30] id, arts. 22, 49 – 54.

[31] Tsvetelina van Benthem, Statement to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ELAC_OEWG_Intervention_-_6_December_2022.pdf.

[32] Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 2021, A/AC.290/2021/CRP.2, para 34; Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of

International Security, 14 July 2021, A/76/135, para 69 et seq.; The Oxford Statement on Ransomware Operations, available at: https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-ransomware-operations/.
[33] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, 141.
[34] Statute of the International Court of Justice, art. 38(1)(b).
[35] Roy Schöndorf, 'Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (EJIL:Talk!, 9 December 2020), available here: https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.
[36] The website of the Ad Hoc Committee is available here: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.
[37] Costa Rica's Position on the Application of International Law in Cyberspace, available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf.
[38] Position available here: https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Appendix_+International+Law+in+Cyberspace+(Statement+by+the+Netherlands).pdf.
[39] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, p. 23 et seq.
[40] Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, 28 May 2021, available at: https://www.mofa.go.jp/files/100200935.pdf.
[41] Government of Canada, International law applicable in cyberspace, available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.
[42] Speech available at: https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
[43] For a detailed examination of the Oxford Process workshops through workshop reports and background papers, see The Oxford Process on International Law Protections in Cyberspace: A Compendium (October 2022), available at: https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf.
[44] Articles on the Responsibility of States for Internationally Wrongful Acts (2001), art. 2.
[45] ECOWAS Directive 1/08/11 on Fighting Cybercrime within ECOWAS.
[46] Arab Convention on Combating Information Technology Offences, adopted in 2010.
[47] T-CY Guidance Note #12: Aspects of ransomware covered by the Budapest Convention, adopted by the 27th Plenary of the T-CY (Strasbourg, 29-30 November 2022).
[48] Id.
[49] Budapest Convention, art. 35.

[50] European Data Protection Supervisor, Opinion 9/2022 on the Recommendation for a Council Decision authorising the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, 18 May 2022, available at: https://edps.europa.eu/system/files/2022-05/2022-05-18-opinion_on_international_convention_en.pdf.
[51] Article 19, Russia: Proposed UN Cybercrime Convention must uphold free speech, 17 February 2022, available at: https://www.article19.org/resources/russia-proposed-un-cybercrime-convention-must-uphold-free-speech/.
[52] UNODC, Future international convention on countering the use of information and communications technologies for criminal purposes FAQ, available at https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/FAQ_on_AHC_September_2023.pdf.
[53] International Convention for the Suppression of the Financing of Terrorism, art. 4 in connection with art. 2.
[54] See, for instance, International Covenant on Civil and Political Rights, 16 December 1966, 999 U.N.T.S. 171.
[55] African Charter of Human and Peoples' Rights, 21 October 1986, 1520 U.N.T.S. 217; American Convention on Human Rights, 22 November 1969, 1144 U.N.T.S. 123; European Convention on Human Rights, 4 November 1950, 213 U.N.T.S. 222.
[56] Human Rights Committee, General Comment 36 on the right to life (2018) at para. 21.
[57] id, para. 26. Emphasis added.
[58] UK Parliament, Ransomware Inquiry, Submission by PwC.
[59] European Court of Human Rights, Öneryıldız v. Turkey, Grand Chamber Judgment, § 90.
[60] See, for instance, Florida House of Representatives, General Bill on Cybersecurity, CS/HB 7055 (2022) - Cybersecurity, available at: https://www.myfloridahouse.gov/Sections/Bills/billsdetail.aspx?BillId=76628.
[61] For an example of discussions in this direction, see National Cyber Security Centre, Solicitors urged to help stem the rising tide of ransomware payments, 8 July 2022, available at: https://www.ncsc.gov.uk/news/solicitors-urged-to-help-stem-the-rising-tide-of-ransomware-payments.
[62] UK Parliament, Ransomware Inquiry, Oral Evidence session.
[63] Corfu Channel (United Kingdom v. Albania), Judgment, 1949 ICJ. 4, at p. 22.
[64] International Law Commission, Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries.
[65] Talita Dias & Antonio Coco, Cyber Due Diligence in International Law (2021), available at: https://elac.web.ox.ac.uk/files/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.
[66] Government of Canada, International law applicable in cyberspace, available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng, para. 33.
[67] ILC, Commentaries to the Articles on State Responsibility, p. 35.
[68] Conduct of organs of a state; Conduct of persons or entities exercising elements of governmental authority; Conduct of organs placed at the disposal of a State by another State; Conduct directed or controlled by a State; Conduct carried out in the absence or default of the official authorities; Conduct of an insurrectional or other movement; Conduct acknowledged and adopted by a State as its own.

[69] ILC, Articles on State Responsibility, art. 7.
[70] Cordula Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians' (2012) 94 International Review of the Red Cross, p. 544.
[71] Matt Burgess, Leaked Ransomware Docs Show Conti Helping Putin From the Shadows (Wired, 18 March 2022), available at: https://www.wired.com/story/conti-ransomware-russia/.
[72] Position of Germany, in Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, 13 July 2021, A/76/136, pp. 39 – 40.
[73] Kristen Eichensehr, Cyberattack Attribution and International Law (JustSecurity, 24 July 2020), available at: https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/.
[74] David Jones, Changing cyber insurance guidance from Lloyd's reflects a market in turmoil (Cybersecurity Dive, 29 August 2022), available at: https://www.cybersecuritydive.com/news/lloyds-cyber-insurance-exclusions/630535/.
[75] Government of Canada, International law applicable in cyberspace, available at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.
[76] Speech available at: https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
[77] Marko Milanović and Michael N. Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic' (2020) 11 Journal of National Security Law & Policy 247.
[78] Mohamed Helal, 'On Coercion in International Law' (2019) 52 NYU Journal of International Law & Policy 65; Harriet Moynihan, The Application of International Law to State Cyberattacks – Sovereignty and Non-Intervention; Tallinn Manual 2.0, rule 66.
[79] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. US), Judgement, 1986 I.C.J, para 202.
[80] Ibid.
[81] Emphasis added. Position available at: https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Appendix_+International+Law+in+Cyberspace+(Statement+by+the+Netherlands).pdf.
[82] Emphasis added. Speech available at: https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
[83] See, for instance, International Covenant on Civil and Political Rights, 16 December 1966, 999 U.N.T.S. 171.
[84] African Charter of Human and Peoples' Rights, 21 October 1986, 1520 U.N.T.S. 217; American Convention on Human Rights, 22 November 1969, 1144 U.N.T.S. 123; European Convention on Human Rights, 4 November 1950, 213 U.N.T.S. 222.
[85] HRC, General Comment 36 on the right to life.
[86] Olivier Corten, *The Law against War: The Prohibition on the Use of Force in Contemporary International Law* (Hart Publishing 2021).
[87] Tom Ruys, 'The meaning of 'force' and the boundaries of the jus ad bellum: are 'minimal' uses of force excluded from UN Charter Article 2(4)?' (2014) 108(2) American Journal of International Law 159; Mary Ellen O'Connell, 'The True Meaning of Force' (2014) 108 AJIL Unbound 141.

[88] Oliver Dörr and Albrecht Randelzhofer, 'Article 2(4)' in Bruno Simma et al (eds), The Charter of the United Nations: A Commentary Vol I (OUP 2012) 208.
[89] Tallinn Manual 2.0, commentary to rule 69, para 9.
[90] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 9 September 2019, p. 7.
[91] CyberLaw Toolkit, Scenario 14: Ransomware campaign, available at: https://cyberlaw.ccdcoe.org/wiki/Scenario_14:_Ransomware_campaign#cite_note-42.
[92] Letter from the Minister of Foreign Affairs of the Netherlands to the President of the House of Representatives, Appendix: International law in cyberspace.
[93] Denmark's Position Paper on the Application of International Law in Cyberspace, July 2023, available at: https://brill.com/view/journals/nord/aop/article-10.1163-15718107-20230001/article-10.1163-15718107-20230001.xml?language=en.
[94] Duncan B. Hollis and Tsvetelina J. van Benthem, 'Threatening Force in Cyberspace', in Laura Dickinson and Edward Berg (eds.), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (Oxford University Press, 2022, Forthcoming)
[95] Josephine Wolff, Who Pays for an Act of Cyberwar? (Wired, 30 August 2022), available at: https://www.wired.com/story/russia-ukraine-cyberwar-cyberinsurance/.
[96] Angus Liu, 'Merck entitled to $1.4B in cyberattack case after court rejects insurers' 'warlike action' claim' (Fierce Pharma, 2 May 2023), available at: https://www.fiercepharma.com/pharma/merck-entitled-14b-payout-cyberattack-case-after-judge-refutes-insurers-warlike-action-claim.
[97] David Jones, 'New Jersey Supreme Court to hear Merck insurance dispute over NotPetya attack' (Cybersecurity Dive, 28 July 2023), available at: https://www.cybersecuritydive.com/news/new-jersey-court-merck-insurers-notpetya/689315/.
[98] Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 2021, A/AC.290/2021/CRP.2, para. 41.
[99] Elisabeth Zoller, Peacetime Unilateral Remedies: An Analysis of Countermeasures (Transnational 1984) 5.
[100] ILC, Articles on State Responsibility, arts. 42 & 48.
[101] Michael Schmitt, 'Estonia Speaks Out on Key Rules for Cyberspace' (JustSecurity, 10 June 2019), available at: https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.
[102] Oxford Process on International Law Protections in Cyberspace: A Compendium, background paper by Przemislaw Roguski.
[103] ILC, Articles on State Responsibility, art. 25.
[104] US Cyber Command, CYBER101 - Defend Forward and Persistent Engagement, 25 October 2022, available at: https://www.cybercom.mil/Media/News/Article/3198878/cyber101-defend-forward-and-persistent-engagement/.
[105] Department of Defence Cyber Strategy 2018: Summary, available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[106] Rieko Miki, Japan to upgrade cyber defense, allowing preemptive measures (NIKKEI Asia, 11 December 2022), available at: https://asia.nikkei.com/Politics/Japan-to-upgrade-cyber-defense-allowing-preemptive-measures.
[107] The Charter of the United Nations uses the language of 'if an armed attack occurs'.